ON THE REDUCTION OF POINTS ON ABELIAN VARIETIES AND TORI

ANTONELLA PERUCCA

Abstract. Let G be the product of an abelian variety and a torus defined over a number field K. Let $R_1, \dots, R_n$ be points in $G(K)$. Let ℓ be a rational prime and let $a_1, \dots, a_n$ be non-negative integers. Consider the set of primes $\mathfrak{p}$ of K satisfying the following condition: the ℓ-adic valuation of the order of $(R_i \bmod \mathfrak{p})$ equals a_i for every $i = 1, \dots, n$. We show that this set has a natural density and we characterize the n-tuples $a_1, \dots, a_n$ for which the density is positive. More generally, we study the ℓ-part of the reduction of the points.

1. Introduction

Let G be the product of an abelian variety and a torus defined over a number field K. Let $\mathcal{O}$ be the ring of integers of K. We reduce G modulo $\mathfrak{p}$, where $\mathfrak{p}$ is a prime of K (a non-zero prime ideal of $\mathcal{O}$). By fixing a model of G over an open subscheme of $\operatorname{Spec}\mathcal{O}$, one can define the reduction $G_\mathfrak{p}$ of G for all but finitely many primes $\mathfrak{p}$ of K. We fix a point R in $G(K)$ and consider its reduction $(R \bmod \mathfrak{p})$, which is well-defined for all but finitely many primes $\mathfrak{p}$ of K (the set of excluded primes depends on the point, unless the toric part of G is trivial). We are interested in the set of values taken by the order of $(R \bmod \mathfrak{p})$, by varying $\mathfrak{p}$.

If R is a torsion point of order n then the order of $(R \bmod \mathfrak{p})$ equals n for all but finitely many primes $\mathfrak{p}$ of K: the excluded primes are either of bad reduction or divide n (bad reduction here means that the reduction is not defined on R or that $G_\mathfrak{p}$ is not the product of an abelian variety and a torus).

Now assume that R has infinite order. Call n_R the number of connected components of the smallest K-algebraic subgroup of G containing R. In [12, Main Theorem] we proved that n_R is the greatest positive integer dividing the order of $(R \bmod \mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of K.

Let ℓ be a rational prime. We study the ℓ-adic valuation of the order of $(R \bmod \mathfrak{p})$. We write ord_ℓ to indicate the ℓ-adic valuation of the order. Let a be a non-negative integer and consider the following set:

$$\Gamma = \{\mathfrak{p} : \ \operatorname{ord}_\ell(R \bmod \mathfrak{p}) = a\}$$

We prove that Γ is finite if $a < v_\ell(n_R)$ and it has a positive natural density if $a \geq v_\ell(n_R)$. See Corollary 19.

For several points we have the following result:

Theorem 1. *Let K be a number field, let $I = \{1, \ldots, n\}$. For every $i \in I$, let G_i be the product of an abelian variety and a torus defined over K and let R_i be a point in $G_i(K)$. Let ℓ be a rational prime. For every $i \in I$, let a_i be a non-negative integer. Consider the following set of primes of K:*

$$\Gamma = \{\mathfrak{p} : \ \forall i \in I \ \ \mathrm{ord}_\ell(R_i \bmod \mathfrak{p}) = a_i\}$$

The set Γ is either finite or it has a positive natural density.

Write $G = \prod_{i=1}^n G_i$ and $R = (R_1, \ldots, R_n)$. Let G_R be the smallest K-algebraic subgroup of G containing R and call G_R^1 the connected component of G_R containing R.

The set Γ is infinite if and only if the following condition is satisfied: there exists a torsion point $T = (T_1, \ldots, T_n)$ in $G_R^1(\bar{K})$ such that $\mathrm{ord}_\ell T_i = a_i$ for every $i \in I$.

Let G be the product of an abelian variety and a torus defined over a number field K. Let R be a point in $G(K)$. Let ℓ be a rational prime and let $\mathfrak{p}$ be a prime of K of good reduction, not over ℓ. Call $a = \mathrm{ord}_\ell(R \bmod \mathfrak{p})$. Let L be a finite Galois extension of K where the points in $G[\ell^a]$ are defined. Then for every prime $\mathfrak{q}$ of L over $\mathfrak{p}$ there exists a unique T in $G[\ell^a]$ such that $\mathrm{ord}_\ell(R - T \bmod \mathfrak{q}) = 0$. We define the ℓ-part of $(R \bmod \mathfrak{p})$ as the $\mathrm{Gal}(\bar{K}/K)$-class of T, which is independent of the choice of $\mathfrak{q}$ and of L.

Theorem 2. *Let G be the product of an abelian variety and a torus defined over K. Let R be a point in $G(K)$. Let ℓ be a rational prime. Let L be a finite Galois extension of K. Let $\mathcal{T}$ be a $\mathrm{Gal}(\bar{K}/K)$-stable subset of $G[\ell^\infty](L)$. Then the following set of primes of K is either finite or it has a positive natural density:*

$$\Gamma = \{\mathfrak{p} : \ \forall \text{ prime } \mathfrak{q} \text{ of } L \text{ over } \mathfrak{p} \ \ \mathrm{ord}_\ell(R - Y \bmod \mathfrak{q}) = 0 \ \text{ for some } Y \text{ in } \mathcal{T}\}$$

Let G_R be the smallest K-algebraic subgroup of G containing R. Call $n_{R,\ell}$ the greatest power of ℓ dividing the number of connected components of G_R. Call G_R^j the connected component of G_R containing the point jR. The set Γ is infinite if and only if $\mathcal{T}$ contains a point in

$$\bigcup_{j \equiv 1 \pmod{n_{R,\ell}}} G_R^j[\ell^\infty](L)$$

Notice that throughout the paper we replace ℓ by a finite set S of rational primes.

To prove the existence of the densities, we apply a method by Jones and Rouse ([9, Theorem 7]). An alternative method is due to Pink and Rütsche, see [15, Chapter 4].

To determine the conditions under which the densities are positive, we refine results of [12] which were based on a method by Khare and Prasad ([10, Lemma 5]). An alternative method is due to Pink, see [14, Theorem 4.1]. Notice that the same method by Khare and Prasad has been applied in the following papers by Banaszak, Gajda, Krasoń, Barańczuk and Górnisiewicz: [1], [3], [7], [2].

Some explicit calculations for the density have been made by Jones and Rouse in [9]. About the order of the reductions of points on the multiplicative group and elliptic curves, see [16] and [5] respectively.

A reason to study the order of the reduction of points is the following. Fix a number field K. Let A be a simple abelian variety defined over K and let R be a point in $A(K)$ of

infinite order. Consider the sequence $\{\mathrm{ord}(R \bmod \mathfrak{p})\}$ indexed by the primes $\mathfrak{p}$ of K (put 1 if the expression is not well-defined). This sequence determines the isomorphism class of A and determines R up to isomorphism. This is a corollary of the results on the support problem ([13, Corollary 8 and Proposition 9]).

2. Preliminaries

Let G be the product of an abelian variety and a torus defined over a number field K. Let R be a point in $G(K)$. Call G_R the smallest K-algebraic subgroup of G containing R, which is the Zariski closure of $\mathbb{Z}R$. The connected component of the identity of G_R is the product of an abelian variety and a torus defined over K (see [12, Proposition 5]). Call it G_R^0. Let n_R be the number of connected components of G_R.

For every finite extension L of K, the smallest L-algebraic subgroup of G containing R is the base change $G_R \times_K \operatorname{Spec} L$. Notice that n_R does not depend on the field L because G_R^0 is geometrically connected (since it has a rational point).

The point $n_R R$ is the smallest positive multiple of R which belongs to G_R^0. There exists a torsion point X in $G_R(\bar{K})$ of order n_R such that $R - X$ belongs to G_R^0 (see [12, Lemma 1]). In particular, the point $n_R X$ is the smallest positive multiple of X which belongs to G_R^0. The group of connected components of G_R is cyclic of order n_R. The connected components of G_R are $G_R^0, \ldots, G_R^{n_R-1}$, where G_R^i is the connected component of G_R containing iR (or equivalentely containing iX).

Lemma 3. *For all but finitely many primes $\mathfrak{p}$ of K, the connected components of $(G_R \bmod \mathfrak{p})$ are $(G_R^i \bmod \mathfrak{p})$ for $i = 0, \ldots, n_R - 1$. In particular, the group of connected components of $(G_R \bmod \mathfrak{p})$ is cyclic of order n_R. If L is a finite Galois extension of K, the analogue properties hold for every prime $\mathfrak{q}$ of L lying outside a finite set of primes of K not depending on L.*

Proof. Let F be a finite Galois extension of K where the points in $G[n_R]$ are defined. Apply [11, Lemma 4.4] to $G[n_R]$ and to $G_R^0[n_R]$. We deduce that for all but finitely many primes $\mathfrak{w}$ of F the following holds: $(n_R X \bmod \mathfrak{w})$ is the smallest positive multiple of $(X \bmod \mathfrak{w})$ which belongs to $(G_R^0 \bmod \mathfrak{w})$. Thus for all but finitely many primes $\mathfrak{p}$ of K the point $(n_R R \bmod \mathfrak{p})$ is the smallest positive multiple of $(R \bmod \mathfrak{p})$ which belongs to $(G_R^0 \bmod \mathfrak{p})$. The first assertion follows.

Let $\mathfrak{q}$ be a prime of L lying over a prime $\mathfrak{p}$ of K. The group of connected components of $(G_R \bmod \mathfrak{q})$ is cyclic of order dividing n_R. Then the second assertion holds since $(G_R \bmod \mathfrak{q})$ is a base change of $(G_R \bmod \mathfrak{p})$, up to discarding a set of primes $\mathfrak{p}$ of K not depending on L. □

Lemma 4 (see also [11, Lemma 4.4])**.** *Let L be a finite Galois extension of K. Let n be a positive integer such that $G[n] \subseteq G(L)$. For every prime $\mathfrak{q}$ of L coprime to n and not lying over a finite set of primes of K (not depending on n nor on L), the reduction modulo $\mathfrak{q}$ gives an isomorphism from $G_R^i[n]$ to $(G_R^i \bmod \mathfrak{q})[n]$ for every $i = 0, \ldots, n_R - 1$.*

Proof. By [11, Lemma 4.4], the property in the statement holds for $G_R^0[n]$ and for $G[n]$. By Lemma 3, up to excluding a finite set of primes $\mathfrak{q}$ (lying over a finite set of primes of K not

depending on n nor on L), we may assume that the connected components of (G_R mod $\mathfrak{q}$) are (G_R^i mod $\mathfrak{q}$) for $i = 0, \ldots, n_R - 1$. We conclude because the reduction modulo $\mathfrak{q}$ maps $G_R^i[n]$ to (G_R^i mod $\mathfrak{q}$)$[n]$. □

Lemma 5 (see also [8, Proposition C.1.5])**.** *Let m be a positive integer. For every $n > 0$ call K_n the smallest extension of K over which the m^n-th roots of R are defined. Then the primes of K which ramify in $\bigcup_{n>0} K_n$ are contained in a finite set.*

Proof. It suffices to prove that there exists a finite set J of primes of K (not depending on n) such that the following holds: every prime $\mathfrak{p}$ of K outside this set does not ramify in K_n. By [11, Lemma 4.4], there exists a finite set J of primes of K (not depending on n) satisfying the following property: for every prime $\mathfrak{p}$ of K outside J and for every prime $\mathfrak{q}$ of K_n over $\mathfrak{p}$, the reduction map modulo $\mathfrak{q}$ is injective on $G[m^n]$. It suffices to show that the inertia group of $\mathfrak{q}$ over $\mathfrak{p}$ is trivial. Let σ be in the inertia group of $\mathfrak{q}$ over $\mathfrak{p}$. Then σ induces the identity automorphism on the reduction modulo $\mathfrak{q}$ of the m^n-th roots of R. Because of the injectivity of the reduction modulo $\mathfrak{q}$ on $G[m^n]$, σ induces the identity automorphism on the m^n-th roots of R hence it is the identity of $\mathrm{Gal}(K_n/K)$. □

3. On the existence of the density

In this section we generalize a result by Jones and Rouse ([9, Theorem 7]). We apply the same method to prove the existence of the natural density.

The results by Pink and Rütsche in [15, Chapter 4] concern the existence of the Dirichlet density. Their method has the advantage (say with respect to Corollary 9) to allow the set $\mathcal{T}$ to be infinite.

Theorem 6. *Let G be the product of an abelian variety and a torus defined over a number field K. Let R be a point in $G(K)$. Let S be a finite set of rational primes and let m be the product of the elements of S. Let T be a point in $G[m^\infty](L)$, where L is a finite Galois extension of K. Call $\mathcal{T}$ the* $\mathrm{Gal}(\bar{K}/K)$*-conjugacy class of T. Then the following set of primes of K has a natural density:*

$$\Gamma = \{\mathfrak{p} : \forall \ell \in S \quad \mathrm{ord}_\ell(R - T \bmod \mathfrak{q}) = 0 \ \textit{for some prime } \mathfrak{q} \textit{ of } L \textit{ over } \mathfrak{p}\}$$
$$= \{\mathfrak{p} : \forall \ell \in S \quad \forall \textit{ prime } \mathfrak{q} \textit{ of } L \textit{ over } \mathfrak{p} \quad \mathrm{ord}_\ell(R - Y \bmod \mathfrak{q}) = 0 \ \textit{for some } Y \textit{ in } \mathcal{T}\}$$

Proof. First step. For every $Y \in \mathcal{T}$, we have $G^0_{R-Y} = G^0_R$ because R and $R - Y$ have a common multiple. Since G^0_R and R are defined over K, it follows that $n_{R-Y} = n_{R-T}$ for every $Y \in \mathcal{T}$. If m and n_{R-T} are not coprime then by [12, Proposition 2] the set Γ is finite and in particular it has density zero. Now assume that m and n_{R-T} are coprime. By replacing R and T by $n_{R-T}R$ and $n_{R-T}T$ respectively, we may assume that for every $Y \in \mathcal{T}$ the algebraic group G_{R-Y} is connected hence equal to G^0_R. Call $G' = G^0_R$, which is the product of an abelian variety and a torus defined over K.

Second step. Let a be such that $m^a(R - Y) = m^a R$ for every $Y \in \mathcal{T}$. In particular, $m^a R$ belongs to G'. Call K_n the smallest extension of K over which the m^{n+a}-th roots of $m^a R$ in G' are defined. By Lemma 5, we may consider only the primes $\mathfrak{p}$ of K which do not ramify in $\bigcup_{n>0} K_n$. We also avoid the primes of bad reduction. By Lemma 4, we may

also assume the following: for every n and for every prime $\mathfrak{w}$ of K_n over $\mathfrak{p}$ the reduction modulo $\mathfrak{w}$ is injective on $G'[m^{n+a}]$. Call $k_{\mathfrak{w}}$ the residue field. Then, for every $Y \in \mathcal{T}$, the reduction modulo $\mathfrak{w}$ induces a bijection from the m^n-th roots of $R-Y$ in G' to the m^n-th roots of $(R - Y \bmod \mathfrak{w})$ in $G'_{\mathfrak{w}}(k_{\mathfrak{w}})$.

By excluding finitely many primes $\mathfrak{p}$ of K, we may also assume that $G_{\mathfrak{w}}$ (respectively $G'_{\mathfrak{w}}$) is the base change of $G_{\mathfrak{p}}$ (respectively $G'_{\mathfrak{p}}$). In particular, we identify $G_{\mathfrak{w}}(k_{\mathfrak{w}})$ (respectively $G'_{\mathfrak{w}}(k_{\mathfrak{w}})$) with $G_{\mathfrak{p}}(k_{\mathfrak{w}})$ (respectively $G'_{\mathfrak{p}}(k_{\mathfrak{w}})$).

Third step. Call H_n the subset of $\mathrm{Gal}(K_n/K)$ consisting of the automorphisms which fix some m^n-th root of $R-Y$ in G' for some $Y \in \mathcal{T}$. We write $\mathrm{Fr}_{\mathfrak{p}}$ for the Frobenius at $\mathfrak{p}$ without specifying the prime of K_n lying over $\mathfrak{p}$.

Since H_n is closed by conjugation, the following set of primes of K is well-defined:

$$B_n = \{\mathfrak{p} \ : \ \mathrm{Fr}_{\mathfrak{p}} \in H_n\}$$

The set B_n has a natural density because of the Cebotarev Density Theorem.

Now we prove that $B_n \supseteq \Gamma$ for every n. Take $\mathfrak{p}$ in Γ and let $\mathfrak{q}$ be a prime of L over $\mathfrak{p}$. Let $Y \in \mathcal{T}$ be such that the order of $(R - Y \bmod \mathfrak{q})$ is coprime to m or equivalently such that the orbit of $(R-Y \bmod \mathfrak{q})$ via the iterates of $[m]$ is periodic. Since $(R \bmod \mathfrak{q})$ belongs to $G_{\mathfrak{p}}(k_{\mathfrak{p}})$ and $(Y \bmod \mathfrak{q})$ is a multiple of $(R \bmod \mathfrak{q})$, the point $(R - Y \bmod \mathfrak{q})$ belongs to $G_{\mathfrak{p}}(k_{\mathfrak{p}}) \cap (G'(L) \bmod \mathfrak{q})$. Then $(R - Y \bmod \mathfrak{q})$ has m^n-th roots in that set for every n. Fix n and let $\mathfrak{w}$ be a prime of K_n over $\mathfrak{q}$. We deduce that there exists Z in $G'(K_n)$ such that $m^n Z = R - Y$ and $(Z \bmod \mathfrak{w})$ is in $G_{\mathfrak{p}}(k_{\mathfrak{p}})$. In particular, Z is fixed by $\mathrm{Fr}_{\mathfrak{p}}$.

Now we suppose that $\mathfrak{p}$ belongs to B_n for infinitely many n and show that $\mathfrak{p}$ belongs to Γ . We have to prove that for every prime $\mathfrak{q}$ of L over $\mathfrak{p}$ there exists $Y \in \mathcal{T}$ such that the orbit of $(R - Y \bmod \mathfrak{q})$ via the iterates of $[m]$ is periodic. Since $\mathcal{T}$ and $G_{\mathfrak{q}}(k_{\mathfrak{q}})$ are finite sets, it suffices to show that for infinitely many n the point $(R-Y \bmod \mathfrak{q})$ has m^n-th roots in $G_{\mathfrak{q}}(k_{\mathfrak{q}})$ for some $Y \in \mathcal{T}$.

Let n be such that $\mathfrak{p}$ belongs to B_n and fix a prime $\mathfrak{w}$ of K_n over $\mathfrak{q}$. Let $Y \in \mathcal{T}$ be such that there exists Z in $G'(K_n)$ satisfying the following properties: $m^n Z = R - Y$ and Z is fixed by $\mathrm{Fr}_{\mathfrak{p}}$. Then $(Z \bmod \mathfrak{w})$ is in $G_{\mathfrak{p}}(k_{\mathfrak{p}})$ and $m^n(Z \bmod \mathfrak{w}) = (R - Y \bmod \mathfrak{w})$. It follows that $(R - Y \bmod \mathfrak{q})$ has m^n-th roots in $G_{\mathfrak{q}}(k_{\mathfrak{q}})$.

Fourth step. For every σ in $\mathrm{Gal}(K_n/K)$, call σ_n (respectively $\sigma_{n,\ell}$) the image of σ in the group of automorphisms of $G'[m^{n+a}]$ (respectively $G'[\ell^{n+a}]$). Notice that the determinant of $\sigma_{n,\ell}$ is an element of $\mathbb{Z}/\ell^{n+a}\mathbb{Z}$ and the fact that the determinant is zero is invariant by conjugation. Then the following set of primes of K is well-defined and it has a natural density because of the Cebotarev Density Theorem:

$$A_n = \{\mathfrak{p} \in B_n \ : \ \det(\mathrm{Fr}_{\mathfrak{p},n,\ell} - \mathrm{id})) \neq 0 \ \ \forall \ell \in S\}$$

We now prove that $A_n \subseteq \Gamma$ for every n. It suffices to show that for every n it is $A_n \subseteq A_{n+1}$ since then A_n is contained in B_n for infinitely many n.

Fix $\mathfrak{p}$ in A_n. Since $\det(\mathrm{Fr}_{\mathfrak{p},n,\ell} - \mathrm{id})) \neq 0$ it follows that $\det(\mathrm{Fr}_{\mathfrak{p},n+1,\ell} - \mathrm{id})) \neq 0$. Furthermore, the image of $(\mathrm{Fr}_{\mathfrak{p},n,\ell} - \mathrm{id})$ in $G'[\ell^{n+a}]$ has the same index as the image of $(\mathrm{Fr}_{\mathfrak{p},n+1,\ell} - \mathrm{id})$ in $G'[\ell^{n+a+1}]$. Thus the m-th roots of the image of $(\mathrm{Fr}_{\mathfrak{p},n} - \mathrm{id})$ belong to the image of $(\mathrm{Fr}_{\mathfrak{p},n+1} - \mathrm{id})$.

For every $Y \in \mathcal{T}$, let P_Y be a m^{n+1}-th root of $R - Y$ in G'. Notice that any other m^{n+1}-th root of $R - Y$ in G' differs from P_Y by an element of $G'[m^{n+1}]$. Then $\mathrm{Fr}_\mathfrak{p}$ is in H_{n+1} if and only if for some $Y \in \mathcal{T}$ the point $\mathrm{Fr}_\mathfrak{p}(P_Y) - P_Y$ is of the form $\mathrm{Fr}_{\mathfrak{p},n+1}(X) - X$ for some X in $G'[m^{n+1}]$. Similarly, because $\mathfrak{p}$ is in H_n, we know that for some Y the point $\mathrm{Fr}_\mathfrak{p}(mP_Y) - mP_Y$ is of the form $\mathrm{Fr}_{\mathfrak{p},n}(X) - X$ for some X in $G'[m^n]$. For such Y, the m-th root $\mathrm{Fr}_\mathfrak{p}(P_Y) - P_Y$ is of the form $\mathrm{Fr}_{\mathfrak{p},n+1}(X) - X$ for some X in $G'[m^{n+1}]$. Thus $\mathrm{Fr}_\mathfrak{p}$ belongs to H_{n+1}. We conclude that $\mathfrak{p}$ belongs to A_{n+1}.

Fifth step. To conclude the proof, we show that the natural density of $B_n \setminus A_n$ goes to zero for n going to infinity. We have:

$$B_n \setminus A_n \subseteq \bigcup_{\ell \in S} \{\mathfrak{p} : \mathrm{Fr}_\mathfrak{p} \in H_n \ ; \ \det(\mathrm{Fr}_{\mathfrak{p},n,\ell} - \mathrm{id})) = 0\}$$

Without loss of generality, we fix ℓ in S and show that the following set (which is well-defined and whose natural density exists by the Cebotarev Density Theorem) has density going to zero for n going to infinity:

$$E_n = \{\mathfrak{p} : \mathrm{Fr}_\mathfrak{p} \in H_n \ ; \ \det(\mathrm{Fr}_{\mathfrak{p},n,\ell} - \mathrm{id})) = 0\}$$

Because of the Cebotarev Density Theorem, the density of E_n is at most the maximum of

$$\frac{\#\{\sigma \in \mathrm{Gal}(K_n/K) : \ \sigma_{n,\ell} = g \, ; \ \sigma \in H_n \, ; \ \det(g - \mathrm{id})) = 0\}}{\#\{\sigma \in \mathrm{Gal}(K_n/K) : \ \sigma_{n,\ell} = g\}}$$

where g varies in the group of the automorphisms of $G'[\ell^{n+a}]$ induced by $\mathrm{Gal}(K_n/K)$.

To estimate the above ratio, we may replace H_n with the subset of $\mathrm{Gal}(K_n/K)$ fixing some ℓ^{n+a}-th root of $m^a R$ in G'. Then we may replace K_n by the smallest extension of K where the ℓ^{n+a}-th roots of $m^a R$ in G' are defined (since the properties of σ are determined by its restriction to this subfield).

By [4, Theorem 2] (applied to the point $m^a R$ in G') there exists a positive integer c, not depending on n nor on g, such that the denominator is at least $\frac{1}{c}\,\#(G'[\ell^{n+a}])$.

Now we estimate the numerator. Let Z be an ℓ^{n+a}-th root of $m^a R$ in G'. Any σ such that $\sigma_{n,\ell} = g$ is determined by $\sigma(Z) - Z$. Since $\sigma \in H_n$, $\sigma(Z) - Z$ is in the image of $g - id$. By the assumptions on g, the cardinality of the image of $g - id$ is at most $\frac{1}{\ell^{n+a}}\,\#(G'[\ell^{n+a}])$. We deduce that the density of E_n is bounded by $\frac{c}{\ell^{n+a}}$. $\square$

Notice that if R is a torsion point then Γ or its complement is a finite set.

Remark 7. *In Theorem 6 it is not necessary to require that the point T has order dividing a power of m.*

Proof. Write $T = T' + T''$ where the order of T' divides a power of m and the order of T'' is coprime to m. Then T'' does not influence the condition defining Γ. $\square$

Remark 8. *In the theorem, if $T = 0$ we have*

$$\Gamma = \{\mathfrak{p} : \forall \ell \in S \quad \mathrm{ord}_\ell(R \bmod \mathfrak{p}) = 0\}$$

Call K_n the smallest extension of K where the m^n-th roots of R are defined. If $G_R = G$, the density of Γ is

$$\lim_{n\to\infty} \frac{\#\{\sigma \in \mathrm{Gal}(K_n/K) : \sigma \textit{ fixes some } m^n\textit{-th root of } R\}}{\#\,\mathrm{Gal}(K_n/K)}$$

Proof. In the proof of the Theorem 6 (in which $a = 0$, $G' = G$), notice that the density of Γ is the limit of the density of B_n. □

Corollary 9. *Let G be the product of an abelian variety and a torus defined over a number field K. Let R be a point in $G(K)$. Let S be a finite set of rational primes. Let $\mathcal{T}$ be a finite $\mathrm{Gal}(\bar{K}/K)$-stable subset of $G(\bar{K})_{\mathrm{tors}}$. Let L be a finite Galois extension of K over which the points in $\mathcal{T}$ are defined. Then the following set of primes of K has a natural density:*

$$\Gamma = \{\mathfrak{p} : \forall \ell \in S \quad \forall \textit{ prime } \mathfrak{q} \textit{ of } L \textit{ over } \mathfrak{p} \quad \mathrm{ord}_\ell(R - Y \bmod \mathfrak{q}) = 0 \textit{ for some } Y \textit{ in } \mathcal{T}\}$$

Proof. The set $\mathcal{T}$ is the disjoint union of the $\mathrm{Gal}(\bar{K}/K)$-orbits of its element. To each orbit we can apply Theorem 6, in view of Remark 7. Then Γ is the disjoint union of finitely many sets admitting a natural density. □

Corollary 10. *Let K be a number field and let $I = \{1, \dots, n\}$. For every $i \in I$ let G_i be the product of an abelian variety and a torus defined over K and let R_i be a point in $G_i(K)$. Let S be a finite set of rational primes. For every $i \in I$, let $\mathcal{T}_i$ be a finite $\mathrm{Gal}(\bar{K}/K)$-stable subset of $G_i(\bar{K})_{\mathrm{tors}}$. Let L be a finite Galois extension of K where the points of $\mathcal{T}_i$ are defined for every i. Then the following set of primes of K has a natural density:*

$$\Gamma = \{\mathfrak{p} : \; \forall \ell \, \forall i \; \; \forall \textit{ prime } \mathfrak{q} \textit{ of } L \textit{ over } \mathfrak{p} \quad \mathrm{ord}_\ell(R_i - Y_i \bmod \mathfrak{q}) = 0 \textit{ for some } Y_i \textit{ in } \mathcal{T}_i\}$$

Proof. Write $G = \prod G_i$ and $R = (R_1, \dots, R_n)$. Call $\mathcal{T}$ the set of points $T = (T_1, \dots, T_n)$ such that $T_i \in \mathcal{T}_i$ for every $i \in I$. Then it suffices to apply Corollary 9 to R and $\mathcal{T}$. □

Corollary 11. *Let K be a number field and let $I = \{1, \dots, n\}$. For every $i \in I$ let G_i be the product of an abelian variety and a torus defined over K and let R_i be a point in $G_i(K)$. Let S be a finite set of rational primes. For every $i \in I$ and for every $\ell \in S$, let $a_{\ell i}$ be a non-negative integer. Consider the following set of primes of K:*

$$\Gamma = \{\mathfrak{p} : \; \forall \ell \in S \;\; \forall i \in I \quad \mathrm{ord}_\ell(R_i \bmod \mathfrak{p}) = a_{\ell i}\}$$

The set Γ has a natural density.

Proof. Call m the product of the elements of S. For every i, let $\mathcal{T}_i$ be the set consisting of the points Y_i in $G_i[m^\infty](\bar{K})$ satisfying $\mathrm{ord}_\ell(Y_i) = a_{\ell i}$ for every $\ell \in S$. Let L be a finite Galois extension of K where the points of $\mathcal{T}_i$ are defined for every i. It suffices to apply Corollary 10 since by Lemma 4, up to excluding finitely many primes $\mathfrak{p}$, we have

$$\Gamma = \{\mathfrak{p} : \; \forall \ell \, \forall i \; \; \forall \textit{ prime } \mathfrak{q} \textit{ of } L \textit{ over } \mathfrak{p} \quad \mathrm{ord}_\ell(R_i - Y_i \bmod \mathfrak{q}) = 0 \textit{ for some } Y_i \textit{ in } \mathcal{T}_i\}$$

□

4. On the positivity of the density

Theorems 1 and 2 are proven respectively in Theorems 14 and 12.

Theorem 12. *Let G be the product of an abelian variety and a torus defined over a number field K. Let R be a point in $G(K)$. Let S be a finite set of rational primes. Call m the product of the elements of S. Let L be a finite Galois extension of K. Let $\mathcal{T}$ be a $\mathrm{Gal}(\bar{K}/K)$-stable subset of $G[m^\infty](L)$. Then the following set of primes of K is either finite or it has a positive natural density:*

$$\Gamma = \{\mathfrak{p} : \forall \ell \in S \quad \forall \text{ prime } \mathfrak{q} \text{ of } L \text{ over } \mathfrak{p} \quad \mathrm{ord}_\ell(R - Y \bmod \mathfrak{q}) = 0 \text{ for some } Y \text{ in } \mathcal{T}\}$$

Let G_R be the smallest K-algebraic subgroup of G containing R. For every ℓ, call $n_{R,\ell}$ the greatest power of ℓ dividing the number of connected components of G_R. Call G_R^j the connected component of G_R containing jR. The set Γ is infinite if and only if the set $\mathcal{T}$ contains a point which can be written as the sum for $\ell \in S$ of elements in

$$\bigcup_{j \equiv 1 \pmod{n_{R,\ell}}} G_R^j[\ell^\infty](L)$$

Proof. The existence of the density was proven in Corollary 9. Since the set Γ increases by enlarging $\mathcal{T}$, we may reduce to the case where $\mathcal{T}$ is the $\mathrm{Gal}(\bar{K}/K)$-orbit of a point T. By [12, Main Theorem] applied to the point $R - T$, the set Γ is infinite if and only if n_{R-T} is coprime to m.

Suppose that Γ is infinite. By [12, Theorem 7] applied to the point $n_{R-T}(R - T)$, there exists a positive density of primes $\mathfrak{p}$ of K such that for some prime $\mathfrak{q}$ of L over $\mathfrak{p}$ it is $\mathrm{ord}_\ell(R - T \bmod \mathfrak{q}) = \mathrm{ord}_\ell(n_{R-T}(R - T) \bmod \mathfrak{q}) = 0$ for every $\ell \in S$. Hence Γ has a positive density.

Write $T = \sum_\ell T_\ell$ where T_ℓ is in $G[\ell^\infty](L)$. Notice that T_ℓ is a multiple of T for every $\ell \in S$. If Γ is infinite, there exist infinitely many primes $\mathfrak{q}$ of L such that $\mathrm{ord}_\ell(R-T \bmod \mathfrak{q}) = 0$. For every $\ell \in S$ the point $(T_\ell \bmod \mathfrak{q})$ is a multiple of $(R \bmod \mathfrak{q})$ hence it belongs to $(G_R \bmod \mathfrak{q})$. By applying Lemma 4 to G and G_R, we deduce that T_ℓ belongs to G_R for every $\ell \in S$. Then to prove the criterion in the statement we may assume that the point T is such that T_ℓ belongs to G_R for every $\ell \in S$.

Notice that n_{R-T} is coprime to ℓ if and only if n_{R-T_ℓ} is coprime to ℓ. To conclude, we show that n_{R-T_ℓ} is coprime to ℓ if and only if the point T_ℓ belongs to $G_R^j[\ell^\infty](L)$ for some $j \equiv 1 \pmod{n_{R,\ell}}$. The last condition is equivalent to saying that $R - T_\ell$ belongs to $G_R^j[\ell^\infty](L)$ for some $j \equiv 0 \pmod{n_{R,\ell}}$.

Let $R - T_\ell$ belong to G_R^j and let X be as in Section 2. Then $G_R^j = G_R^0 + jX$ and the smallest multiple of jX lying in G_R^0 is $[n_R/(n_R, j)]jX$. Since $G_{R-T_\ell}^0 = G_R^0$, we deduce that n_{R-T_ℓ} is coprime to ℓ if and only if $n_R/(n_R, j)$ is coprime to ℓ. This is equivalent to saying that $j \equiv 0 \pmod{n_{R,\ell}}$. □

Corollary 13. *Let K be a number field, let $I = \{1, \ldots, n\}$. For every $i \in I$, let G_i be the product of an abelian variety and a torus defined over K and let R_i be a point in $G_i(K)$. Let S be a finite set of rational primes. Call m the product of the elements of S. Let L be a*

finite Galois extension of K. For every i, let $\mathcal{T}_i$ be a $\mathrm{Gal}(\bar{K}/K)$-stable subset of $G_i[m^\infty](L)$. Then the following set of primes of K is either finite or it has a positive natural density:

$$\Gamma = \{\mathfrak{p} : \forall i \ \ \forall \ell \ \ \forall \textit{ prime } \mathfrak{q} \textit{ of } L \textit{ over } \mathfrak{p} \quad \mathrm{ord}_\ell(R_i - Y_i \bmod \mathfrak{q}) = 0 \textit{ for some } Y_i \textit{ in } \mathcal{T}_i\}$$

Write $G = \prod_{i=1}^n G_i$ and $R = (R_1, \ldots, R_n)$. Let G_R be the smallest K-algebraic subgroup of G containing R. For every ℓ, call $n_{R,\ell}$ the greatest power of ℓ dividing the number of connected components of G_R. Call G_R^j the connected component of G_R containing jR. Let $\mathcal{T}$ be the product of the $\mathcal{T}_i$ for $i \in I$. The set Γ is infinite if and only if the set $\mathcal{T}$ contains a point which can be written as the sum for $\ell \in S$ of elements in

$$\bigcup_{j \equiv 1 \pmod{n_{R,\ell}}} G_R^j[\ell^\infty](L)$$

Proof. Notice that

$$\Gamma = \{\mathfrak{p} : \ \forall \ell \in S \ \ \forall \textit{ prime } \mathfrak{q} \textit{ of } L \textit{ over } \mathfrak{p} \quad \mathrm{ord}_\ell(R - Y \bmod \mathfrak{q}) = 0 \textit{ for some } Y \textit{ in } \mathcal{T}\}$$

Then it suffices to apply Theorem 12. □

Theorem 14. *Let K be a number field, let $I = \{1, \ldots, n\}$. For every $i \in I$, let G_i be the product of an abelian variety and a torus defined over K and let R_i be a point in $G_i(K)$. Let S be a finite set of rational primes. For every $i \in I$ and for every $\ell \in S$, let $a_{\ell i}$ be a non-negative integer. Consider the following set of primes of K:*

$$\Gamma = \{\mathfrak{p} : \ \forall \ell \in S \ \ \forall i \in I \quad \mathrm{ord}_\ell(R_i \bmod \mathfrak{p}) = a_{\ell i}\}$$

The set Γ is either finite or it has a positive natural density.

Write $G = \prod_{i=1}^n G_i$ and $R = (R_1, \ldots, R_n)$. Let G_R be the smallest K-algebraic subgroup of G containing R. For every ℓ, call $n_{R,\ell}$ the greatest power of ℓ dividing the number of connected components of G_R. Call G_R^j the connected component of G_R containing jR.

The set Γ is infinite if and only if one of the following equivalent conditions is satisfied:

- **(i):** *for every $\ell \in S$ there exists a torsion point $T_\ell = (T_{\ell 1}, \ldots, T_{\ell n})$ such that $\mathrm{ord}_\ell(T_{\ell i}) = a_{\ell i}$ for every $i \in I$ and T_ℓ belongs to*

$$\bigcup_{j \equiv 1 \pmod{n_{R,\ell}}} G_R^j[\ell^\infty]$$

- **(ii):** *for every $\ell \in S$ there exists a torsion point $T_\ell = (T_{\ell 1}, \ldots, T_{\ell n})$ in $G_R^1(\bar{K})$ such that $\mathrm{ord}_\ell(T_{\ell i}) = a_{\ell i}$ for every $i \in I$.*

Lemma 15. *In Theorem 14, suppose that condition (ii) is satisfied. Then there exists a torsion point $T = (T_1, \ldots, T_n)$ in $G_R^1(\bar{K})$ such that $\mathrm{ord}_\ell(T_i) = a_{\ell i}$ for every $i \in I$ and for every $\ell \in S$.*

Proof. For every $\ell \in S$, the torsion point $T_\ell - X$ belongs to $G_R^0(\bar{K})$. Then we can write $T_\ell - X = Z_\ell + Z'_\ell$, where Z_ℓ is a point in $G_R^0[\ell^\infty]$ and Z'_ℓ is a torsion point in $G_R^0(\bar{K})$ of

order coprime to ℓ. Define $T=\sum_\ell Z_\ell + X$. The point T is a torsion point in $G_R^1(\bar{K})$. For every $\ell \in S$ and for every $i \in I$ we have:

$$\operatorname{ord}_\ell(T_i)=\operatorname{ord}_\ell(\sum_\ell Z_{\ell i}+X_i)=\operatorname{ord}_\ell(Z_{\ell i}+X_i)=\operatorname{ord}_\ell(Z_{\ell i}+Z'_{\ell i}+X_i)=\operatorname{ord}_\ell(T_{\ell i})=a_{\ell i}$$

□

Proof of Theorem 14. The existence of the density for Γ was proven in Corollary 11.

Call m the product of the elements of S. Let L be a finite Galois extension of K where the points in $G_i[\ell^{a_{\ell i}}]$ are defined for every $\ell \in S$ and for every $i \in I$. We may assume (see Lemma 4) that for every prime $\mathfrak{q}$ of L the reduction modulo $\mathfrak{q}$ gives a bijection from $G_i[\ell^{a_{\ell i}}]$ to $(G_i[\ell^{a_{\ell i}}] \bmod \mathfrak{q})$, for every $\ell \in S$ and for every $i \in I$.

Let $\mathcal{T}$ be the set consisting of the points $Y=(Y_1,\dots,Y_n)$ in $G[m^\infty]$ such that $\operatorname{ord}_\ell(Y_i)=a_{\ell i}$ for every $\ell \in S$ and for every $i \in I$. Notice that $\mathcal{T}$ is contained in $G[m^\infty](L)$ and it is $\operatorname{Gal}(\bar{K}/K)$-stable. A prime $\mathfrak{p}$ of K belongs to Γ if and only if for every prime $\mathfrak{q}$ of L over $\mathfrak{p}$ the following holds: for some $Y \in \mathcal{T}$ $\operatorname{ord}_\ell(R-Y \bmod \mathfrak{q})=0$ for every $\ell \in S$. Apply Theorem 12 to R and $\mathcal{T}$. We deduce that the set Γ is infinite if and only if it has a positive density. We also deduce that Γ is infinite if and only if $\mathcal{T}$ contains a point $T=(T_1,\dots,T_n)$ with the following property: we can write $T=\sum_\ell T_\ell$ where for every $\ell \in S$ the point T_ℓ is in $G_R^j[\ell^\infty](L)$ for some $j \equiv 1 \pmod{n_{R,\ell}}$. Notice that $\mathcal{T}$ contains such an element if and only if condition (i) is satisfied.

Suppose again that Γ is infinite. We show that condition (ii) is satisfied. Without loss of generality, fix $\ell \in S$. Because of condition (i) there exists $T_\ell=(T_{\ell 1},\dots,T_{\ell n})$ such that $\operatorname{ord}_\ell(T_{\ell i})=a_{\ell i}$ for every $i \in I$ in $G_R^j[\ell^\infty](L)$ for some $j \equiv 1 \pmod{n_{R,\ell}}$. Let X be as in section 2 and notice that the order of $(j-1)X$ is coprime to ℓ. Since $G_R^j(\bar{K})=G_R^1(\bar{K})+(j-1)X$ we deduce that $T_\ell-(j-1)X$ is in $G_R^1(\bar{K})$ and satisfies the properties of condition (ii).

Viceversa, suppose that condition (ii) is satisfied. By Lemma 15, there exists a torsion point $T=(T_1,\dots,T_n)$ in $G_R^1(\bar{K})$ such that $\operatorname{ord}_\ell(T_i)=a_{\ell i}$ for every $i \in I$ and for every $\ell \in S$. In particular, the point $R-T$ belongs to $G_R^0(\bar{K})$. Furthermore, $G_{R-T}^0=G_R^0$ since R and $R-T$ have a common multiple. We deduce that G_{R-T} is connected.

Let F be a finite Galois extension of K where T is defined. By applying [12, Theorem 7] to the point $R-T$, we find infinitely many primes $\mathfrak{p}$ of K such that for some prime $\mathfrak{w}$ of F over $\mathfrak{p}$ it is $\operatorname{ord}_\ell(R-T \bmod \mathfrak{w})=0$ for every $\ell \in S$.

Up to excluding finitely many primes $\mathfrak{p}$, we may assume that the order of $(T_i \bmod \mathfrak{w})$ equals the order of T_i for every $i \in I$.

Then such primes $\mathfrak{p}$ belong to Γ since for every $\ell \in S$ and for every $i \in I$ it is

$$\operatorname{ord}_\ell(R_i \bmod \mathfrak{p})=\operatorname{ord}_\ell(R_i \bmod \mathfrak{w})=\operatorname{ord}_\ell(T_i \bmod \mathfrak{w})=\operatorname{ord}_\ell T_i=a_{\ell i}$$

□

Suppose that in Theorem 14 every G_i and every R_i is non-zero. Then the condition $G_R=G$ implies that for every choice of the parameters $a_{\ell i}$ the set Γ is infinite. The condition $G_R=G$ is equivalent to saying that R generates a free $\operatorname{End}_K G$-submodule of

$G(K)$, see [12, Remark 6]. The following example shows that the set Γ may be infinite for every choice of the parameters even if $G_R \neq G$.

Example 16. Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication and such that $E(\mathbb{Q})$ contains three points P_1, P_2 and P_3 which are $\mathbb{Z}$-linearly independent. For example consider the curve $[0,0,1,-7,6]$ of [6]. Let $I = \{1,2\}$ and let $S = \{\ell\}$. Let $G_1 = G_2 = E^2$. Consider the points $R_1 = (P_1, P_3)$ and $R_2 = (P_2, P_3)$. Let a_1 and a_2 be non-negative integers. There exist infinitely many primes $\mathfrak{p}$ such that $\mathrm{ord}_\ell(R_i \bmod \mathfrak{p}) = a_i$ for $i = 1,2$. Indeed, the point (P_1, P_2, P_3) is independent in E^3 so we can apply [12, Proposition 12]. Thus we find infinitely many $\mathfrak{p}$ such that $\mathrm{ord}_\ell(P_i \bmod \mathfrak{p}) = a_i$ for $i = 1,2$ and $\mathrm{ord}_\ell(P_3 \bmod \mathfrak{p}) = 0$.

Remark 17. *Suppose that the number of connected components of G_R is coprime to ℓ. Then in condition (ii) of Theorem 14 it suffices to require that T_ℓ is in G_R and not necessarily in G_R^1. In general, it suffices to require that T_ℓ is in G_R^b for some b coprime to ℓ.*

Proof. Let X be as in section 2. If the number of connected components of G_R is coprime to ℓ then the order of X is coprime to ℓ. Then by summing to T_ℓ a multiple of X we may assume that T_ℓ is in G_R^1. For the second assertion, notice that $G_R^b = G_{bR}^1$. So by applying Theorem 14 to the point bR we find infinitely many primes $\mathfrak{p}$ of K such that for every $i \in I$ and for every $\ell \in S$ it is

$$\mathrm{ord}_\ell(R_i \bmod \mathfrak{p}) = \mathrm{ord}_\ell(bR_i \bmod \mathfrak{p}) = a_{\ell i}$$

We deduce that the set Γ is infinite. $\square$

Remark 18. *With the notations of Theorem 14, for every $\ell \in S$ define the following set:*

$$\Gamma_\ell = \{\mathfrak{p} \in K : \ \forall i \in I \quad \mathrm{ord}_\ell(R_i \bmod \mathfrak{p}) = a_{\ell i}\}$$

We have $\Gamma = \cap_\ell \Gamma_\ell$ and Γ is an infinite set if and only if Γ_ℓ is an infinite set for every $\ell \in S$.

Proof. In Theorem 14, condition (ii) is a collection of conditions for every $\ell \in S$. $\square$

For one point of infinite order we have:

Corollary 19. *Let G be the product of an abelian variety and a torus defined over a number field K. Let R be a point in $G(K)$ of infinite order. Let S be a finite set of rational primes. For every $\ell \in S$ let a_ℓ be a non-negative integer. Consider the following set of primes of K:*

$$\Gamma = \{\mathfrak{p} : \ \forall \ell \in S \quad \mathrm{ord}_\ell(R \bmod \mathfrak{p}) = a_\ell\}$$

The set Γ is either finite or it has a positive natural density. Let G_R be the smallest K-algebraic subgroup of G containing R and call n_R the number of connected components of G_R. Then Γ is infinite if and only if for every ℓ in S it is $a_\ell \geq v_\ell(n_R)$. Furthermore, n_R is the greatest positive integer dividing the order of $(R \bmod \mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of K.

Proof. The assertions are consequences of [12, Main Theorem] and Corollary 11. □

Notice that $G^1_R(\bar{K})$ contains a torsion point of order n if and only if n is a multiple of n_R. This follows from the fact that $G^1_R(\bar{K}) = X + G^0_R(\bar{K})$, where X is as in Section 2.

Acknowledgements

I thank Rafe Jones and Jeremy Rouse for helpful discussions. I thank Peter Jossen, Emmanuel Kowalski and Dino Lorenzini for useful comments.

References

[1] G. Banaszak, W. Gajda, and P. Krasoń, *Detecting linear dependence by reduction maps*, J. Number Theory **115** (2005), no. 2, 322–342.

[2] G. Banaszak and P. Krasoń, *On arithmetic in Mordell-Weil groups*, arXiv:0904.2848.

[3] S. Barańczuk, *On reduction maps and support problem in K-theory and abelian varieties*, J. Number Theory **119** (2006), no. 1, 1–17.

[4] D. Bertrand, *Galois Representations and Transcendental Numbers*, New Advances in Trascendence Theory (Durham, 1986), 37–55, Cambridge Univ. Press, Cambridge, 1988.

[5] J. Cheon and S. Hahn, *The Orders of the Reductions of a Point in the Mordell-Weil Group of an Elliptic Curve*, Acta Arith. **88** (1999), no. 3, 219–222.

[6] J. Cremona, *Elliptic Curve Data*, http://www.warwick.ac.uk/staff/J.E.Cremona/

[7] W. Gajda and K. Górnisiewicz, *Linear dependence in Mordell-Weil groups*, J. Reine Angew. Math. **630** (2009), 219–233.

[8] M. Hindry and J. H. Silverman, *Diophantine Geometry. An Introduction*, Graduate Texts in Mathematics 201, Springer Verlag, New York, 2000.

[9] R. Jones and J. Rouse, *Iterated Endomorphisms of Abelian Algebraic Groups*, arXiv:0706.2384.

[10] C. Khare and D. Prasad, *Reduction of homomorphisms mod p and algebraicity*, J. Number Theory, **105** (2004), no. 2, 322–332.

[11] E. Kowalski, *Some local-global applications of Kummer theory*, Manuscripta Math. **111** (2003), no. 1, 105–139.

[12] A. Perucca, *Prescribing valuations of the order of a point in the reductions of abelian varieties and tori*, J. Number Theory **129** (2009), no. 2, 469–476.

[13] A. Perucca, *Two variants of the support problem for products of abelian varieties and tori*, J. Number Theory **129** (2009), no. 8, 1883–1892.

[14] R. Pink, *On the order of the reduction of a point on an abelian variety*, Math. Ann. **330** (2004), no. 2, 275–291.

[15] E. Rütsche, *Über das Reduktionsverhalten von Punkten auf abelschen Varietäten*, Master thesis at ETH Zürich, March 2004, http://www.math.ethz.ch/~pink/Theses/Master.html

[16] A. Schinzel, *Primitive divisors of the expression $A^n - B^n$ in algebraic number fields*, J. Reine Angew. Math. **268/269** (1974), 27–33.

Antonella Perucca
EPFL Station 8, CH-1015, Lausanne, Switzerland

antonella.perucca@epfl.ch